КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-04 34 06 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 3.0

Программа генерации ключей mkkey. Руководство по использованию

СЕИУ.00009-04 34 06
Листов 13

Литера О

2019

Аннотация

Настоящий документ содержит руководство по использованию программы mkkey из состава «МагПро КриптоПакет» 3.0.

Содержание

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа mkkey из комплекта «МагПро КриптоПакет» 3.0 выполняет создание закрытых ключей для использования в программном комплексе «МагПро КриптоПакет» 3.0, в том числе создание ключей на аппаратных носителях.

Поддерживаются аппаратные носители Вьюга, Rutoken S, Rutoken ЭЦП.

Программа не формирует заявки на получение сертификата. Для формирования заявок необходимо использовать команду req утилиты openssl.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

2 УСЛОВИЯ РАБОТЫ ПРОГРАММЫ

Для инициализации клавиатурного ДСЧ, запроса пароля к ключевому контейнеру и сообщения пользователю о необходимых действиях с аппаратными устройствами программа использует текстовый интерфейс.

Задание режимов работы (например, параметры алгоритмов и набор генерируемых ключей) выполняется с помощью опций командной строки.

В случае использования клавиатурной генерации файла инициализации программного ДСЧ программа не должна запускаться в ssh-сессии.

Программа предназначена для работы в следующих операционных системах:

Windows 7 SP1/8.1/10;
Windows Server 2008R2 SP1/2012/2012R2/2016;
Debian GNU/Linux 7(wheezy)/8(jessie)/9(stretch);
Linux Mint 17.x, 18.x, Linux Mint Debian Edition 2;
Ubuntu 14.04, 16.04;
RedHat Enterprise Linux 6, 7;
CentOS 6, 7;
SUSE Linux 11, 12;
OpenSUSE 42.2, 42.3;
OS EMIAS 1.0;
Альт Линукс 6, 7, 8;
МСВСфера Сервер 6.3, МСВСфера АРМ 6.3;
Атликс 3.1;
Гослинукс IC4;
FreeBSD 10.x, 11.x;
Oracle Solaris 10, 11;
MacOS 10.12;
Rosa Enterprise Desktop (RED) X2, X3;
Rosa Enterprise Linux Server (RELS) 6, 7;
РОСА КОБАЛЬТ 1.0;
Astra Linux Special Edition РУСБ.10015-07.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3 ФУНКЦИИ ПРОГРАММЫ

Программа предоставляет удобный пользовательский интерфейс для выполнения операций по созданию закрытых ключей и ключей подписи и их записи на ключевой носитель, а также формирования файла инициализации программного датчика случайных чисел.

Программа не выполняет указанные операции самостоятельно, а лишь обеспечивает взаимодействие с пользователем. Для формирования ключей вызывается утилита openssl. Для формирования файла инициализации программного ДСЧ вызывается утилита mkseed.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

4 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» 3.0

Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» 3.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» 3.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0. Правила пользования» (СЕИУ.СЕИУ.00009–04 94).

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5 УСТАНОВКА И НАСТРОЙКА ПРОГРАММЫ

Программа устанавливается и настраивается автоматически при установке утилиты openssl (см. «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0. Утилита openssl. Руководство по использованию», СЕИУ.00009-04 34 03).

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6 ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ

6.1 Формат запуска программы

Формат запуска программы:

```
mkkey [опции]
```

По умолчанию (если не указаны опции) программа выводит краткую справку об опциях.

6.2 Опции

```
-V              - отобразить номер версии программы
-r [имя файла] - запись файла инициализации программного ДСЧ
                  если имя файла не указано, будет использован файл
  /home/abra/.magprocryptopack/random_seed

-a              - алгоритм ключа, по умолчанию gost2012_256
-n              - не шифровать ключ
-p <параметр>   - набор параметров для ключа (умолчание - A)
-w <имя файла> - файл, в который будет записан закрытый ключ
-t <носитель>   - записать ключ(и) на носитель указанного типа
                  поддерживаются носители: VJUGA, RUTOKEN
-y              - удалить ключ(и) с аппаратного носителя
-c <имя файла> - использовать файл конфигурации openssl
-K <имя файла> - использовать ключ из указанного файла (DER-формат)

Только для носителя VJUGA:
 -s <параметр> - набор параметров для ключа подписи (умолчание - A)
 -x <параметр> - набор параметров для ключа шифрования (умолчание - XA)

Только для носителя RUTOKEN:
 -k <номер>     - идентификационный номер ключа
 -P             - защищать ключ PIN-кодом
```

6.3 Выбор алгоритма

Программа mkkey предоставляет возможность создания ключей подписи и обмена для алгоритма ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 (последний - только для целей совместимости с предыдущими версиями).

6.4 Выбор файла инициализации ДСЧ

При создании ключей программа создает файл инициализации программного ДСЧ, что позволяет дальнейшую эксплуатацию OpenSSL с выбранным ДСЧ.

Если в момент запуска программы не указан параметр опции -r, то создаётся файл инициализации с умолчательным именем:

В ОС Windows — `%APPDATA%\MagProCryptoPack\random_seed`

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

В POSIX-системах — `$HOME/.magprocryptopack/random_seed`

В случае использования клавиатурного ДСЧ также возможно явное указание имени файла инициализации. Имя файла указывается в качестве значения параметра -r.

6.5 Инициализация ДСЧ

В случае использования клавиатурного датчика случайных чисел программа предлагает пользователю последовательно вводить с клавиатуры указанные символы: латинские буквы и цифры. Ввод осуществляется группами по 5 символов (последняя группа может быть короче). В начале каждой строки приглашения ввода символов в скобках выводится количество введенных символов и общее количество требуемых символов, разделенных косой чертой. В случае некорректного ввода количество требуемых символов увеличивается.

6.6 Ввод пароля

Для отказа от зашифрования ключевых контейнеров на пароле необходимо при запуске программы указать опцию -n.

Если опция -n при запуске программы не была указана, перед инициализацией ДСЧ программа требует дважды ввести пароль для защиты ключевых контейнеров длиной от 6-ти символов до 32 символов.

Для отмены ввода пароля следует ввести пустой пароль, т.е. нажать Enter, не вводя никаких символов.

В пароле могут быть использованы как символы ASCII, так и русские буквы. Русские буквы интерпретируются как имеющие кодировку UTF-8, что соответствует рекомендациям PKCS#5. Следует обратить внимание, что OpenSSL и большая часть приложений, её использующих, не производит никаких преобразований кодировки пароля. Поэтому ключи, защищенные паролем, состоящим из русских букв, могут быть использованы с командно-строчной утилитой openssl и большинством приложений библиотеки OpenSSL только при запуске последних в локали UTF-8.

6.7 Создание контейнеров на аппаратном носителе

6.7.1 Выбор аппаратного носителя

Ключевые контейнеры на аппаратных носителях создаются в тех случаях, если указана опция -t со значением VJUGA или RUTOKEN. Запись ключевых контейнеров производится на соответствующее устройство.

Не предполагается работа с несколькими устройствами одного типа одновременно.

6.7.2 Работа с ключами на устройстве Вьюга

Устройство Вьюга позволяет хранить только два ключа.

При создании ключей на устройстве Вьюга всегда создаётся два ключа - ключ подписи и ключ шифрования. По умолчанию эти ключи имеют параметры шифрования A и XA. Альтернативные параметры могут быть указаны с помощью опций -s и -x, например:

```
mkkey -t VJUGA -s C -x XB
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6.7.3 Работа с ключами на устройстве Rutoken

Устройство Rutoken позволяет хранить несколько ключей в пределах доступной памяти устройства. Каждому ключу назначается десятичное число в интервале от 1 до 65535 - идентификационный номер. При создании ключа требуется указать идентификационный номер, который будет назначен создаваемому ключу, например:

```
mkkey -t RUTOKEN -k 20
```

В этом случае будет создан ключ с идентификатором 20, при дальнейшей работе с этим ключом (например, с помощью утилиты openssl) следует использовать его спецификацию: RUTOKEN:20

Если на токене уже имеется ключ с указанным идентификатором, вновь созданный ключ заменит старый.

Для защиты ключа PIN-кодом следует использовать опцию -P. В этом случае для чтения ключа с устройства будет требоваться ввод PIN-кода пользователя.

7 СОЗДАНИЕ ЗАЯВОК НА ПОЛУЧЕНИЕ СЕРТИФИКАТА

7.1 Краткие сведения о команде *req* утилиты openssl

Программа mkkey создает только закрытый ключ.

Для получения сертификата на соответствующий открытый ключ необходимо сформировать заявку на ключ с помощью команды *req* утилиты openssl.

Внимание. На каждый ключ создаётся отдельная заявка.

Команда *req* позволяет вводить информацию, которая должна содержаться в заявке, с клавиатуры, либо считывать её из конфигурационного файла.

Если в полях сертификата должны присутствовать русские буквы, вводить информацию с клавиатуры следует в кодировке utf-8.

Формат вызова команды *req* при использовании PKCS#8-контейнеров (содержащихся в файлах):

```
openssl req -new [-config файл-конфигурации] -key файл-pkcs8\
 -out имя-файла-заявки
```

Формат вызова команды *req* при использовании аппаратного контейнера:

```
openssl req -new [-config файл-конфигурации] -key спецификация-ключа \
 -keyform ENGINE -engine cryptocom -out имя-файла-заявки
```

Спецификация ключа, хранящегося в аппаратном контейнере, может быть одной из перечисленных:

Ключ подписи на устройстве Вьюга:

```
VJUGA.S
```

Ключ шифрования на устройстве Вьюга:

```
VJUGA.X
```

Ключ на устройстве Rutoken с идентификатором <номер>:

```
RUTOKEN:<номер>
```

Более подробная информация по ключам команды *req* приведена в документе «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0. Утилита openssl. Руководство по использованию», СЕИУ.00009-04 34 03.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий сопроводительного докум. и дата	Подпись	Дата
Изм.	измененных	замененных	новых	аннулированных					

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения